Lunar Testbed for Demonstrating Deep-Space Optical Communications, Ranging and Secret Key Distribution

Victor A. Vilnrotter,* Matthew D. Thill,* and Daniel J. Hoppe†

ABSTRACT. — Stars are currently used to evaluate the pointing performance of the Hybrid Radio Frequency (RF)/Optical receiver, but stars are not suitable for communications, ranging, and science applications. We propose to create modulated artificial optical sources on the Moon by illuminating one or more of the five Apollo retro-reflectors from the ground, using existing resources. This will ensure the continued development and testing of optical communications, ranging, and science protocols suitable for deep-space applications at the conclusion of the Psyche mission. Realistic planetary rotation and orbital trajectories, atmospheric turbulence, and signal power commensurate with the photon-starved deep-space optical channel will be made possible due to the "inverse distance-to-the-fourth" power law characteristic of radar reflections.

I. Introduction

The Deep Space Network's (DSN) Hybrid RF/Optical receiver is an entirely new concept in optical communications. In its final configuration, it will employ sixty-four (64) hexagonal mirrors with spherical shape placed on the main reflector of a 34 m DSN antenna at the Goldstone Deep Space Communications Complex. This segmented optical configuration is equivalent to an 8.3-meter diameter direct detection receiver, designed for deep-space optical communications. This incredible NASA asset will be available for further demonstrations and experiments when the planned Psyche mission concludes. The unique design of the Hybrid RF/Optical receiver enables novel applications for enhanced communications, ranging, and science applications that will greatly benefit NASA's exploration of the solar system, the Kuiper belt, and beyond.

Although most lunar retro-reflector experiments to date have been carried out at 532 nm and 1064 nm wavelengths, the Psyche spacecraft carries a 4-watt 1550 nm laser as the downlink optical transmitter for telemetry. For the examples in this paper, we assume that a spare version of this laser transmitter, or a working engineering model, could be used to illuminate the Apollo retro-reflectors from the ground, generating a weak return signal to

* Communications Architectures and Research Section.

† Communications Ground Systems Section.

The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

emulate a photon-starved deep-space channel. We would then be able to carry out communications, ranging, and secret key distribution (SKD) experiments on the ground, in order to advance the development of future deep-space photonic protocols.

II. The Optical Lunar Retro-Reflector Link

The key components of the ground-to-Moon optical lunar retro-reflector link is characterized by a laser transmitter on the ground, transmitting pulse-position modulated (PPM) pulses to one of the Apollo retro-reflectors. The retro-reflector array reflects the intercepted portion of the laser beam back towards the transmitter, and the ground receiver collects a portion of the reflected photons for processing.

A conceptual design of the ground system is shown in Figure 1, which is an artist's rendition of the Hybrid RF/Optical Antenna located at the Venus site in the Goldstone Deep-Space Communications Complex at Ft. Irwin, California. We propose using a spare optical transmitter from the Psyche spacecraft, or a suitable engineering model of this optical transmitter located on the ground next to the optical receiver, together with a laser safety monitoring system, to generate the PPM modulated 1550 nm laser signal to illuminate the lunar retro-reflectors.

The 34-m Hybrid RF/Optical Antenna is currently under development. When completed, there will be 64 hexagonal optical mirrors, with a spherical instead of parabolic or hyperbolic figure, arranged in four groups symmetrically around the main reflector of the antenna. The equivalent circular area of this array is 8.3 meters. While the collecting area of this receiver is equivalent to that of a single 8.3-meter mirror, its resolution is not the same, since the 1-m mirror elements are not phased up coherently. Therefore, the diffraction-limited field-of-view (FOV) of this receiver cannot exceed that of a single 1-m mirror, which would ideally be λ/d radians as the physical limit, where λ is the

Figure 1. Artist's conception of the 34-meter Hybrid RF/Optical Antenna.

wavelength. However, the mirrors are not diffraction limited, hence their FOV is actually much larger, in part determined by the accuracy of the alignment between the mirror elements. The receiver will use a 64-element wide bandwidth photon-counting nanowire detector array with quantum efficiency of up to 90% or more, hence capable of counting individual photons. During operation, the FOV of the receiver is adjusted to $\theta_{rec} = 1.8\lambda/r_0$, where r_0 is the Fried parameter, characterizing the coherence-length of the atmosphere, which is an indication of the degree of turbulence.

The Uplink Channel. The Psyche transmitter assembly is envisioned as the ground-based uplink transmitter that illuminates the Apollo retro-reflectors, which introduce enough loss into the channel upon reflection to emulate a photon-starved deep-space link, including real-world effects such as relative motion between the transmitter and receiver, predict-driven pointing and point-ahead compensation at the transmitter, acquisition and tracking of the lunar retro-reflector signal by the receiver, temporal synchronization of weak PPM signals, detection and decoding of the transmitted data, and the application of ranging and science demonstration experiments to test new SKD algorithms and relativistic tests of gravity effects. A major advantage of the lunar testbed is that round-trip light-time between the Earth and the Moon is only 2.6 seconds, instead of tens of minutes to hours as in deep-space links, enabling much faster evaluation and testing of new concepts.

The Downlink Channel. The Apollo 15 retro-reflector, the largest of the Apollo retro-reflectors left on the Moon, consists of 300 solid fused silica corner cubes, uncoated and not silvered, hence capable of reflecting a large band of optical and infrared wavelengths including 632 nm red, 1064 nm near-infrared Ng-YAG laser light, as well as 1550 nm infrared light currently used in optical fiber-optic communications links. A schematic of the Apollo 15 retro-reflector is shown in Figure 4, which shows the arrangement of the 300 corner-cubes on two panels, the larger panel with $17 \times 12 = 204$ and the smaller panel with $8 \times 12 = 96$ corner-cubes.

The non-coherently reflected laser signal power reaching the ground has unique properties that are not immediately obvious, and hence need to be examined in greater detail for the lunar testbed application. First, we consider a scalar model that accounts for diffraction to determine the reflected signal power density reaching the ground. Second, the polarization properties of the corner-cubes that are important in the context of SKD that employ polarization basis, such as the BB84 protocol, will be considered.

Atmospheric Beam-Steering on the Uplink Beam. The transmitted uplink laser beam must pass through the terrestrial atmosphere, which often experiences random fluctuations in refractive index due to thermal effects and wind, called turbulence. The impact of turbulence on optical beam propagation is generally characterized by the Fried parameter r_0, which defines the coherence-length of an optical wavefront passing through the turbulent atmosphere.

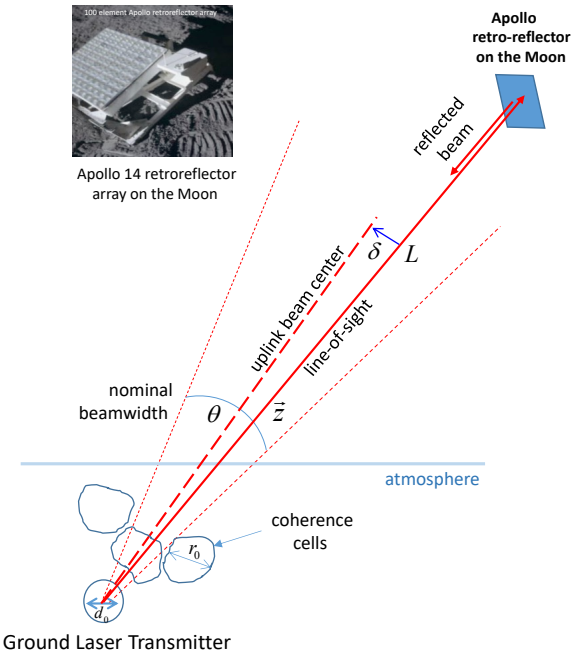

Figure 2. Diagram of uplink beam and lunar retro-reflector array, with the standard deviation of the beam-steering angle δ smaller than the beam divergence.

The Fried parameter r_0 is often defined at 500 nm wavelengths, where strong turbulence is characterized by $r_0 \leq 3$ cm, moderate turbulence by $r_0 \cong 5$ cm, and weak turbulence by $r_0 \geq 7$ cm. The Fried parameter is a function of wavelength, and can be extrapolated from the measurement wavelength λ_0 to another wavelength λ_1 via the relation $r_0(\lambda_1) \cong r_0(\lambda_0)(\lambda_1/\lambda_0)^{6/5}$. For example, if $r_0 = 3$ cm at 500 nm wavelength corresponding to strong turbulence, then at 1550 nm the Fried parameter becomes $r_0(1550) \cong 11.7$ cm. The correction factor for these two frequencies is $(1550/500)^{6/5} = 3.887$, hence for moderate turbulence at 1550 nm r_0 becomes 19.4 cm, and for weak turbulence it is approximately 27.2 cm.

Consider an uplink transmitter with telescope diameter d_0. If the beam divergence is greater than the standard deviation of the random beam-steering due to turbulence, then fades at the target can be minimized. This situation is illustrated in Figure 2, where the standard deviation of the random beam-steering angle δ is smaller than the beam divergence, minimizing random fades at the retro-reflector. For a Gaussian beam with beam-waist w_0, it has been shown in Reference [1] that if the ratio of Gaussian beam diameter $2w_0$ to Fried parameter r_0 is in the range $0.35 \leq 2w_0 \,/\, r_0 \leq 1.22$, then the impact of ground turbulence on the uplink beam is primarily random beam-steering, and the intensity scintillation index σ_I^2 can be characterized by the following model in the far-field: $\sigma_I^2 = 4\alpha^2 \,/\, (1 + 4\alpha)$, where $\alpha \cong 0.863(2w_0 \,/\, r_0)^{5/3}$ for lunar distances. For $2w_0/r_0 = 0.5$ direct substitution yields $\alpha = 0.2718$, and the scintillation index becomes $\sigma_I^2 = 0.14$, which implies relatively small intensity fluctuations at the lunar target.

Note that other techniques can be applied to mitigate fading, such as splitting the laser power into several beams and then separating the beams spatially to undergo independent fading, which can average the fades at the target. Alternately, adaptive optics techniques can be employed to minimize beam steering by turbulence, but these techniques are beyond the scope of this study. Here we consider system parameters that enable minimal beam-steering by expanding the uplink beam sufficiently to minimize turbulence effects, but without the additional complexities of more sophisticated system concepts.

Background Effects in Lunar Retro-Reflector Applications. There are several scenarios suitable for lunar retro-reflector applications, including nighttime operation during the new Moon when the Apollo 15 site is dark, nighttime operation with the Apollo 15 site in sunlight generating a bright lunar background, and daytime operation for these two cases with strong, nominal, and weak atmospheric turbulence.

Atmospheric turbulence impacts both the uplink and the downlink, but in different ways. On the uplink channel, the transmitted laser light is steered by turbulence leading to fading at the retro-reflector as the beam occasionally misses the target, whereas on the downlink it increases the point spread function (PSF) of the received reflected laser signal, forcing the receiver to open up its FOV, thus admitting more background photons into the receiver that degrades communications and ranging performance.

First, we consider the uplink channel and suggest an approach to mitigate beam-steering due to atmospheric turbulence. Second, the magnitude of the backscattered laser radiation and background radiation due to solar illumination will be considered. Finally, the impact of the Apollo 15 retro-reflector corner-cubes on the polarization of the uplink signal will be evaluated, which is important for implementing some of the SKD algorithms considered in this study.

Background effects for the lunar retro-reflector experiments: backscattered laser signal counts. Here we develop a simple model that can be used to approximate the laser radiation backscattered from the lunar surface in the vicinity of the Apollo 15 retro-reflector array. In the far-field, the divergence of the transmitted beam is given by $\Omega = 2\lambda/\pi w_0$. If we assume a Gaussian beam waist of $w_0 = 10$ cm and hence beam diameter of 20 cm at the telescope aperture (consistent with the Psyche telescope diameter of 22 cm), then $\Omega = 2\lambda/\pi w_0 \cong 10\mu$ radians. At the lunar distance of $R = 384400 \times 10^3$ m, the diameter of the circular footprint is $\Omega R = 3.844 \times 10^3$ m, with an illuminated footprint area of $A_{M,fp} = \pi(3.844 \times 10^3)^2/4 = 1.18 \times 10^7 \mathrm{m}^2$. With an average uplink laser power of $P_u = 4$ watts, the power density at the Moon is $\Phi_M = 3.4 \times 10^{-7}$ watts per square meter. Assuming the reflection coefficient (or albedo) α of the lunar surface near the Apollo 15 site is approximately at 1550 nm is $\alpha \cong 0.1$, and that the lunar surface scattering is Lambertian, we approximate the reflected power as being backscattered towards the Earth uniformly into a $\pm\pi/4$ radian cone, yielding a footprint diameter of $D_{E,fp} = 2R\sin(\pi\ /\ 4) = 5.44 \times 10^8$ m at the distance of the Earth R, and an effective scattering area of $A_{E,fp} = \frac{\pi}{4} D_{E,fp}^2 = 2.32 \times 10^{17} \mathrm{m}^2$.

Taking the reflectivity coefficient into account, the scattered laser power density at the ground is $\Phi_E = \alpha P_u / A_{E,fp} = 1.72 \times 10^{-18}$ watts per square meter. The Hybrid RF/Optical receiving antenna has an effective optical diameter of $D_{rec} = 8.3$ m, or an effective collecting area of $A_{rec} = \frac{\pi}{4} D_{rec}^2 = 54.1$ square meters. At a laser wavelength of 1550 nm, the energy of a single photon is $E_{ph} = hc / \lambda = 1.28 \times 10^{-19}$ joules, where h is Planck's constant. Therefore, the number of backscattered laser photons collected from the Apollo 15 region by the ground receiver is $n_{sc} = \Phi_E A_{rec} / E_{ph} = 728$ photons per second. Assuming the maximum PPM slot-width generated by the transmitter is $\tau = 8$ ns, the average number of backscattered laser photons per PPM slot is approximately $N_{sc} = \tau n_{sc} = 5.8 \times 10^{-6}$ photons per slot. This suggests that backscattered laser photons can be neglected at the ground receiver, when 8 ns PPM slots are used. This, however, may not be the case when lunar-orbiting satellites illuminate the retro-reflector for ranging application, due to the much shorter distance of lunar orbiters to the Moon.

Background effects for the lunar retro-reflector experiments: background counts from the full Moon. When the Apollo 15 lander region is illuminated by direct sunlight, the reflected solar photons encompass the solar spectrum at wavelengths shorter than 3 microns, but begin to deviate at longer wavelengths due to blackbody radiation from the 390 K illuminated lunar surface. The spectral radiance of the full Moon is shown in Figure 3, where it can be seen that the spectral radiance of the full Moon at a wavelength of 1.55 microns is roughly 20 watts per square meter, steradian, and optical filter bandwidth in micro-meters [2].

The effective diameter of the Hybrid RF/Optical receiver is $D_{rec} = 8.3$ meters, and its effective area is $A_{rec} = 54.1$ square meters. It is common practice with the Hybrid RF/Optical receiver to use an FOV of $\theta_{rec} = 1.8\lambda / r_0 = 2.79 \times 10^{-5}$ radians with $r_0 = 10$ cm and $\lambda = 1550$ nm, or a solid angle of approximately $\Omega_{rec} = \frac{\pi}{4} \theta_{rec}^2 = 6.1 \times 10^{-10}$ steradians. Assuming a 1 Angstrom optical filter with a bandwidth of 10^{-4} micro-meters is used, the total background power impinging on the photon-counting detector when

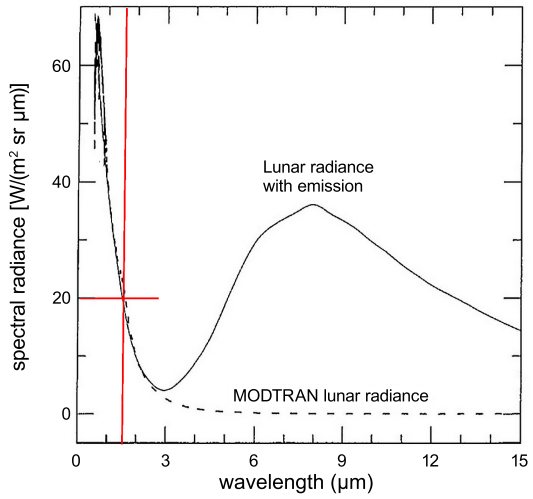

Figure 3. Spectral radiance of the full Moon outside the Earth's atmosphere, including both solar reflection and thermal emission, as illustrated in [2].

pointing at the full Moon is approximately $P_M = 6.6 \times 10^{-11}$ watts under the stated conditions. Using these numbers, the average number of photons per second when pointing at the full Moon is approximately $n_M = P_M \,/\, E_{ph} = 5.16 \times 10^8$ photons per second, or $N_{sc} = \tau n_{sc} = 4.12$ photons per slot, when looking at the full Moon with strong turbulence. This is likely to be the strongest background radiation that would be encountered during well-designed retro-reflector experiments, corresponding to $r_0 =$ 10 cm at 1550 nm, which represents poor seeing or strong turbulence. Under excellent seeing conditions corresponding to Fried parameters of up to $r_0 = 30$ cm at 1550 nm wavelength, the background photon-counts will be approximately one tenth of the results shown here. Based on these calculations, the number of background photons can range from near zero photons per PPM slot, to as much as four photons per slot under the extreme conditions of the full Moon and strong turbulence. These background counts suggest that lunar retro-reflector experiments should either be carried out at night, or under excellent seeing conditions when the Apollo site is not fully illuminated by the Sun, in order to minimize background radiation. The impact of background radiation on the detection of uncoded M-PPM symbols is discussed in Section IV, Deep Space Communications Example.

Scalar Model of the Apollo 15 Retro-Reflector. In the Apollo 15 retro-reflector array, the diameter of each corner-cube is $d_{cc} = 3.8$ cm. The pattern of corner-cubes is shown in Figure 4, consisting of a smaller $12 \times 8 = 96$ element corner-cube array, and a larger $12 \times 17 = 204$ element array for a total of 300 corner-cubes. The array was placed on the Moon's surface with the normal to the plane of the array pointing towards the Earth, to within a few degrees, to maximize the projected area of the array. Each corner-cube was carefully aligned prior to deployment; however, the surfaces were not aligned to a small fraction of an optical wavelength, hence the reflections do not add coherently. Therefore, each corner-cube reflects a plane-wave that diffracts at an angle of roughly λ/d_{cc} radians, generating the corresponding far-field patterns on the downlink. The diffracted field components add non-coherently in the far-field, resulting in a received downlink signal power 300 times greater than the power from each corner-cube. In other words, the total reflected power is determined by the effective area of the array, but this power diffracts into a wide angle of λ/d_{cc} radians determined by the corner-cube diameter, rather than by the much larger dimensions of the array.

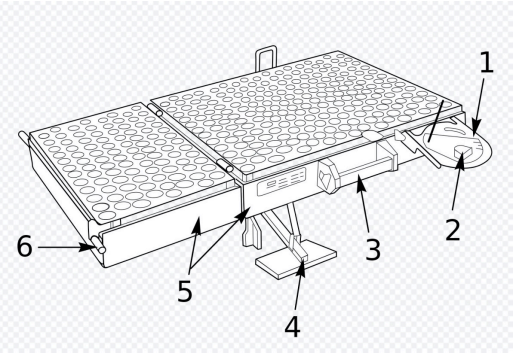

Figure 4. Schematic diagram of the Apollo 15 retro-reflector array, including labels for handle, pods, panels, and other mechanical components.

The reflected power density can be determined by computing the diameter $D_{E,cc}$ of the footprint on the ground, due to the circular corner-cubes with diameter $d_{cc} = 0.038$ m: $D_{E,cc} = R\lambda \,/\, d_{cc} = 15.68 \times 10^3$ meters, or 15.68 km. Using the value of the power density on the Moon derived previously, $\Phi_M = 3.4 \times 10^{-7}$ watts per square meter assuming transmitter power of 4 watts and $r_0 \cong 10$ cm, and assuming an effective area of $A_{rr} = \frac{\pi}{4} 300 \times d_{cc}^2 = 0.33$ meters, the reflected power at the Moon is $P_{M,rr} = \Phi_m A_{rr} = 1.16 \times 10^{-7}$ watts. With an effective ground footprint area of $A_{E,fp} = \frac{\pi}{4} D_{E,cc}^2 = 1.93 \times 10^8$ square meters, this yields the following power density on the ground: $\Phi_E = P_{M,cc} \,/\, A_{E,fp} = 6.01 \times 10^{-16}$ watts per square meter. Using the previously determined value of photon energy at 1550 nm, $E_{ph} = hc \,/\, \lambda = 1.28 \times 10^{-19}$, and the area of the Hybrid RF/Optical receiver $A_{rec} = 54.1$ square meters, the average number of photons captured by the receiver aperture is $N_s = \Phi_E A_{rec} \,/\, E_{ph} = 2.54 \times 10^5$ photons per second, under poor atmospheric conditions corresponding to $r_0 \cong 10$ cm. Under nominal conditions, when the Fried parameter is 20 cm, four times as many photons would be received on the average, yielding $N_s \cong 1.016 \times 10^6$ or in round numbers approximately a million photons per second.

III. Polarization Effects in the Apollo 15 Retro-Reflector

Polarization Effects: The Apollo 15 lunar retro-reflector is composed of solid, uncoated, fused silica corner-cubes that rely on total internal reflection. The relationship between the polarization of the incident electromagnetic field components (E_{x0}, E_{y0}) and the reflected field components (E_x, E_y) can be expressed in terms of the Jones matrix $[J]$ as described in [3], shown in Equation (1):

$$\begin{pmatrix} E_x \\ E_y \end{pmatrix} = [J] \begin{pmatrix} E_{x0} \\ E_{y0} \end{pmatrix}, \tag{1}$$

where the electric field components are in the (x, y) plane perpendicular to the direction of propagation, here assumed to be normally incident on the solid retro-reflector (SRR) as shown in Figure 5. The azimuthal angle is denoted by α, and in general the reflected components will also differ by an angle φ, which implies that linear polarization is converted to elliptical polarization.

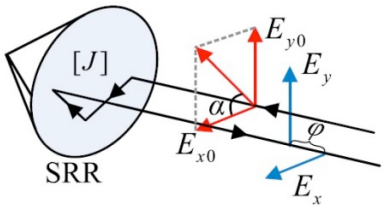

Figure 5. Geometry of incident and reflected electrical field components impinging a solid retro-reflector, characterized by a Jones matrix, as illustrated in [3].

The calculation of the Jones matrix involves the refractive index of the optical material used in the corner-cube. The refractive index of fused silica used in the Apollo 15 retro-reflector at 632.8 nm is 1.45702, which is the value used to compute the Jones matrix in [3]. The following values are also reported for several optical materials in Table 1 of Reference [3]:

Table 1. Jones matrices for several common optical materials, from [3].

Material	Refractive Index (@ 632.8 nm)	Jones Matrix
CaF_2	1.43289	$\begin{bmatrix} -0.5871 - 0.7268i & 0.2521 - 0.0354i \\ -0.2521 + 0.0354i & -0.3644 + 0.8604i \end{bmatrix}$
Fused Silica	1.45702	$\begin{bmatrix} -0.7087 - 0.6015i & 0.2487 - 0.0782i \\ -0.2487 + 0.0782i & -0.2369 + 0.8989i \end{bmatrix}$
ULE	1.48093	$\begin{bmatrix} -0.7945 - 0.4737i & 0.2393 - 0.1158i \\ -0.2393 + 0.1158i & -0.1215 + 0.9170i \end{bmatrix}$
BK-7	1.51509	$\begin{bmatrix} -0.8697 - 0.2962i & 0.2188 - 0.1610i \\ -0.2188 + 0.1610i & 0.0242 + 0.9185i \end{bmatrix}$

The complex entries in the Jones matrix along with the unequal diagonal elements implies that for linearly polarized input vectors, for example X and Y, the reflected waves will be orthogonal elliptically polarized waves. For these output waves the polarization ellipses are rotated 90 degrees with respect to each other and the electric field vector rotates around in the right hand sense for one of the outputs and in the left hand sense for the other.

Consider the application of these concepts to secret key distribution, as described in Section VI. The eigenvectors of the Jones matrix represent the two particular orthogonal polarizations that will reproduce themselves upon reflection from the cube. The "+" and "–" bases in the BB84 protocol can be created by choosing two orthogonal combinations of the eigenvectors. Assume the eigenvectors are represented as $(0,1)$, and $(1,0)$, respectively. An example BB84 protocol could employ the eigenvectors themselves as the "+" set, while the "–" set could be chosen as $\frac{1}{\sqrt{2}}(1,1)$, and $\frac{1}{\sqrt{2}}(1,-1)$. Other choices are also possible using different pairs of linear combinations of the eigenvectors. Each design choice has implications for the complexity of the polarizing components; some resulting in simpler polarizing components on transmit while others would have simpler receive components.

IV. Deep-Space Communications Example

An important application of the Lunar Retro-Reflector Testbed will be the emulation of the deep-space channel, due to the "inverse range-to-the-fourth power" loss characteristic of radar systems, while including realistic propagation effects from the atmosphere and orbital dynamics. The huge space loss between the ground laser transmitter and the ground receiver, via the lunar retro-reflector channel, mimics space loss from several astronomical units (AU), however it does not suffer from long round-trip light-times (RTLT) associated with real interplanetary channels, which can be from 10 minutes to

several hours or more. Since the RTLT between the Earth and the Moon is only 2.6 seconds, this enables testing, evaluation and modification of new detection, ranging, and science experiments rapidly, enabling a large number of runs per scheduled track instead of just one. First, we consider a communications emulation example, using realistic models for the Hybrid RF/Optical receiver and spacecraft laser transmitter developed for the Psyche spacecraft after that mission is over in 2023.

The signal model employed by the Deep Space Optical Communications (DSOC) transmitter provides a good example of the parameters used in the following discussion. The DSOC transmitter assembly takes binary data as input blocks, encodes the data, and converts it to PPM symbols with M slots according to the block diagram shown in Figure 6, from Reference [4]. Binary information blocks are input to a pseudo-noise randomizer, after which CRC bits and termination bits are added, then input to a serially concatenated PPM encoder to generate PPM symbols that are further input to a channel interleaver forming frames. A frame synchronization marker is added in after each frame, the symbols are repeated q times, after which the symbols are mapped into PPM slots.

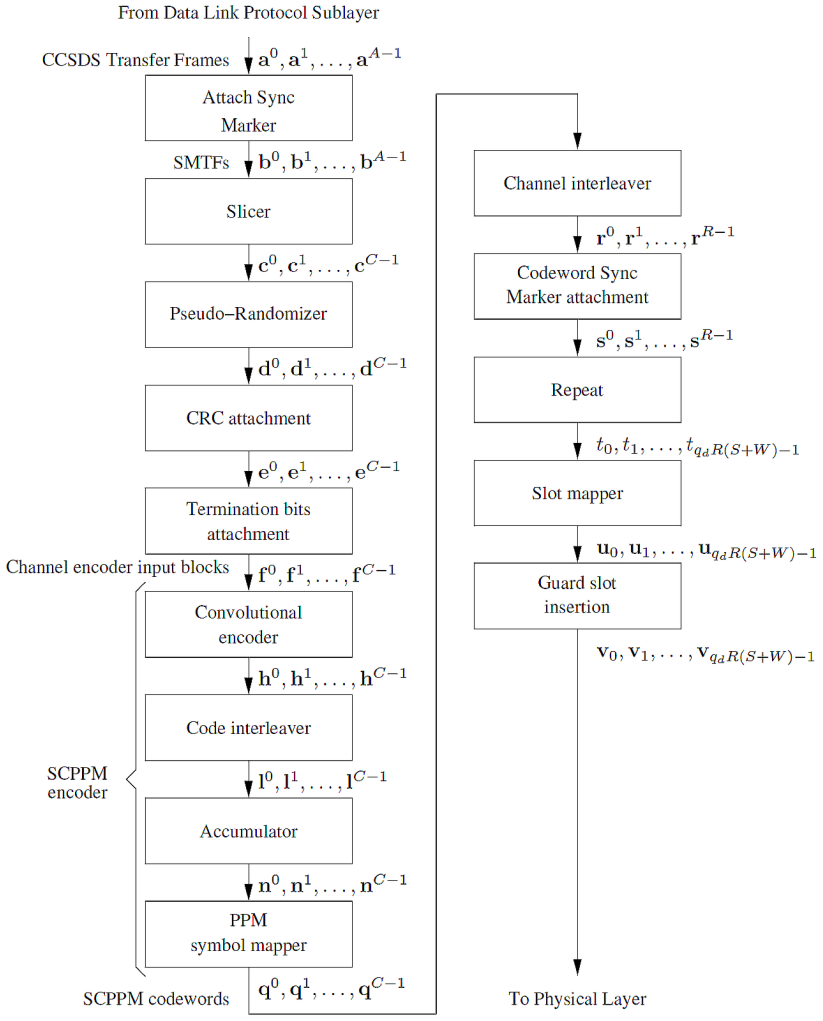

Figure 6. Signal flow diagram of DSOC transmitter defining the downlink signal format, to be used as the uplink in this application.

In addition, M/4 guard slots are added to each PPM symbol, generating pseudo-PPM symbols of (M + M/4) slots. This is the uplink and downlink signal format that will be used in the simulations [5].

Note that repetition coding can be used to increase the slot-width by a factor of $q = 1, 2, \ldots, 32$, thus increasing the effective signal power per slot, at the expense of PPM symbol-rate.

Poisson model of received PPM symbols. For the simulation, the downlink serially concatenated PPM (SCPPM) symbols have been generated using a Matlab encoder developed by Kenneth Andrews (JPL, Section 332) which was used in the simulation to generate PPM symbols of order (16, 32, 64, or 128).

It is noteworthy that the electrical signal in the optical photon-counting receiver is very different in nature from the signal in a RF receiver, where due to much lower carrier frequency, the number of photons is so great that the intensity function of the received pulse is reproduced accurately. By contrast, the intensity function in the photon-counting receiver is approximated by a number of discrete high-bandwidth pulses.

Figure 7 shows three examples of SCPPM pulses with photon counts for the case of $M = 16$, and 256 high-rate simulation samples per pulse illustrating high energy pulses with $\lambda_s = 0.05$ photons per sample yielding an average of 12.8 photons per pulse without background, low energy pulses with $\lambda_s = 0.005$ photons per sample yielding an average of 1.28 photons per pulse, and low energy pulses with a moderate background photon rate of $\lambda_b = 0.005$, showing background photons occurring randomly between the received signal pulses.

The examples of Figure 7 represent the photon-counts that can be generated by a wideband photon-counting detector, which can effectively resolve 256 time-intervals per 8 ns PPM pulse, approximating the “best case” scenario for estimating pulse-edge time of arrival. However, the deep-space receiver developed for DSOC samples at a maximum rate of 2 Gsps, generating 16 samples per 8 nsec PPM pulse [5]. In the following, we compare the ideal case of ultra-high rate sampling (256 samples per 8 ns pulse approximating arbitrarily high sampling rates), with the performance of the DSOC receiver, for estimating the range of the Apollo 15 retro-reflector from the ground.

Although deep-space signals are typically encoded using forward error corrections codes (FEC) to improve performance, there are many different coding schemes including the SCPPM developed at JPL. One of the goals of the lunar testbed concept is to enable the development and testing of new FEC protocols and decoding strategies for future applications.

It is generally accepted that FEC and decoder performance is related to uncoded symbol-error or bit-error probabilities, hence we use the uncoded probability of bit error (PBE) to indicate the feasibility of testing under various signal and background conditions. Note that in communications applications, the M/4 intersymbol guard-slots are not used to make a symbol decision since it can be assumed that slot, symbol, and frame synchronization has been established before symbol detection begins, hence the location of the information-bearing slots and guard slots are known and can be ignored.

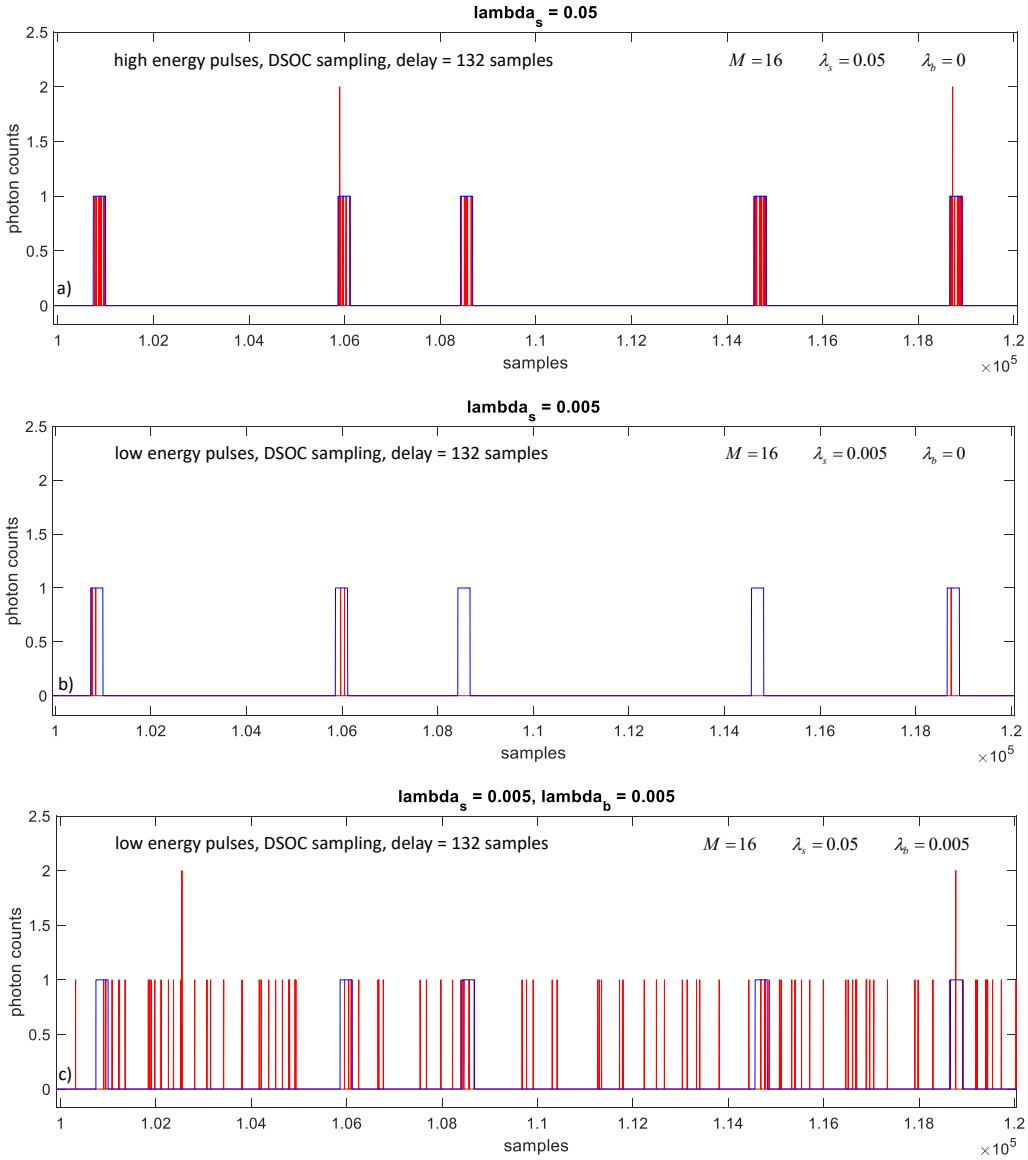

Figure 7. Examples of SCPPM photon counts with M=16, 256 high-rate simulation samples per pulse: a) no background, high energy pulses; b) no background, low energy pulses; and c) moderate background showing random background photons between signal pulses.

The PBE is related to the probability of PPM symbol error (PSE), as $PBE = \frac{M}{2} PSE \; / \; (M-1)$, which states that if a PPM symbol is in error, then for large M roughly half of the bits are in error. The maximum likelihood algorithm for detecting PPM symbols in the Poisson channel calls for counting the received photons in each of the M information-bearing slots, and select the largest count as the best estimate of the signal-slot location. In the absence of background, the probability of correctly guessing the signal slot is just the probability that at least one photon is detected. With Poisson statistics and an average of K_S signal photons per slot, the probability of detecting at least one photon in the signal slot is given by $P(C) = p(k > 0) = 1 - \exp(-K_s)$, where k is the number of photons and $\exp(-K_s) = p(k = 0)$. If zero photons are observed in all of the slots, then a random

choice can be made which yields correct detection 1 out of M times on the average. In this case, the probability of correct detection is given by $\frac{1}{M}\exp(-K_s)$. The general expression for correct symbol detection in the presence of background photons with average number of K_b photons per slot is shown in Equation (2),

$$P(C) = \sum_{r=0}^{M-1} \frac{1}{r+1} \binom{M-1}{r} \sum_{k=1}^{\infty} \frac{(K_s+K_b)^k}{k!} \exp[-(K_s+K_b)] \left[\frac{K_b^k}{k!}\exp(-K_b)\right]^r \left[\sum_{j=0}^{k-1} \frac{K_b^j}{j!}\exp(-K_b)\right]^{M-1-r}$$

$$+ M^{-1}\exp[-(K_s + MK_b) \tag{2}$$

where the last expression represents the case of zero observed photons over all M slots, in the presence of background. The expression in Equation (2) includes the case of all possible r-fold equalities. However, it was found that for large M, and especially in the presence of background photons, equalities do not contribute significantly to correct detection, hence equalities can generally be ignored. With this approximation the probability of correct detection is the probability that for any count k, the signal slot containing $(K_s + K_b)$ photons exceeds the remaining $(M-1)$ slots containing only background photons K_b:

$$P(C) \cong \sum_{k=1}^{\infty} \frac{(K_s+K_b)^k}{k!} \exp[-(K_s+K_b)] \left[\sum_{j=0}^{k-1} \frac{K_b^j}{j!}\exp(-K_b)\right]^{M-1} . \tag{3}$$

For large M, the approximate probability of bit error is given by $PBE \cong \frac{1}{2}[1 - P(C)]$.

Figure 8 shows several examples of the achievable bit error probabilities, PBE, as a function of average signal photons per slot, for average background energies of $(K_b = 0, 0.1, 1, 4)$ photons per slot, assuming Poisson statistics in the received photons. These background energies represent nighttime viewing of the Apollo 15 region without solar illumination $(K_b = 0)$, light and moderate background due to morning/evening or daytime viewing of the Apollo 15 region $(K_b = 0.1,1)$, and worst-case background conditions due to a fully illuminated Moon $(K_b = 4)$.

The red circles in Figure 8 represent average signal slot-counts received from the Apollo 15 retro-reflector for Fried parameters of $r_0 = 3, 5, 7$ cm representing strong, medium, and weak turbulence, for PPM symbols of length $M + \frac{M}{4}$ slots that include the guard-slots, and for repetition order $q = 4$, which means that each PPM symbol is repeated q times to increase the average signal energy per longer equivalent combined slots. Note that the background energy also increases by a factor of q, but in the optical domain with Poisson statistics, increasing the signal energy at a fixed ratio of signal-to-background photons yields improved performance. This is not the case for radio frequency systems with additive Gaussian noise, where performance depends only on the signal-to-noise ratio.

With modern FEC coding and decoding algorithms, the required performance of $PBE \leq 10^{-6}$ can usually be achieved when the uncoded bit-error probabilities are less than 0.1. We can therefore consider the nominal region below the dashed line in Figure 8 as the

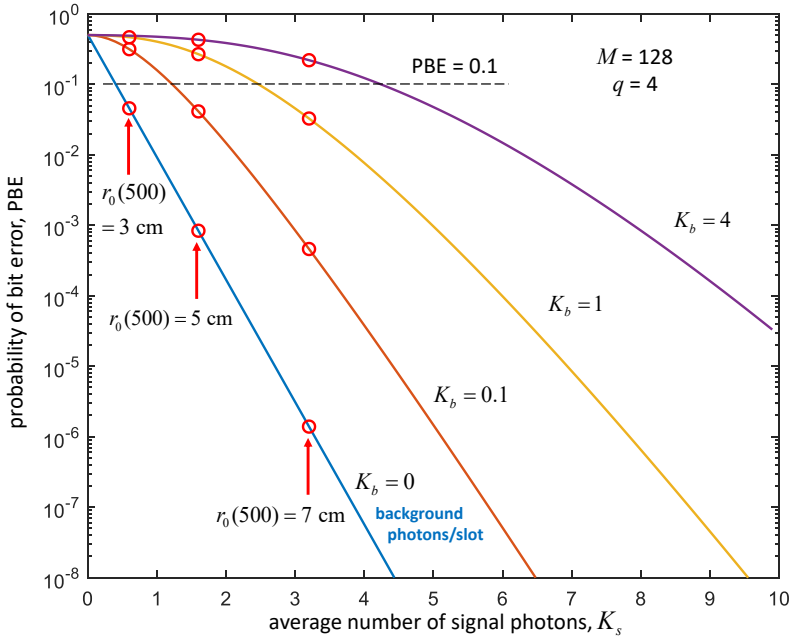

Figure 8. Probability of bit error as a function of the average number of signal photons per slot, for a range of background energies relevant to the lunar retro-reflector application: q = 4.

"region of validity" for communications and related experiments, when $M = 128$ PPM symbols and $q = 4$ repetition factors are used. It can be seen that with negligible background noise, even strong turbulence that requires expanding the uplink beam to reduce fading at the Apollo 15 retro-reflector, useful experiments can still be carried out according to the above criterion. It was found that smaller *M* and fewer repetitions lead to significantly degraded performance, hence the largest available values of *M* should be used on the uplink.

With low to moderate background, $K_b = 0.1$ to 1, nominal performance can be achieved

with moderate to weak turbulence, but not with strong turbulence when $M = 128$ and $q = 4$. However, with the worst-case background corresponding to the full Moon, $K_b = 4$, it is not possible to achieve nominal PBE performance even under weak turbulence conditions.

V. Delay and Range Estimation via Correlation

An example of a sequence of PPM symbols with *M* = 16 and with 8 ns slots (using 16 transmitter samples of 500 ps each), and in addition using 16 "simulation samples" per "transmitter sample" to enable near-continuous representation of the range-induced delay, is shown in Figure 9. The asterisks represent 500 ps transmitter samples used in the DSOC receiver, by averaging the transmitter samples to obtain 16 samples per chip.

Figure 9 shows the average photon intensity per received pulse, for the transmitted pulses (blue) and the simulated received pulses (red) modulo the PN code, with a fractional-chip

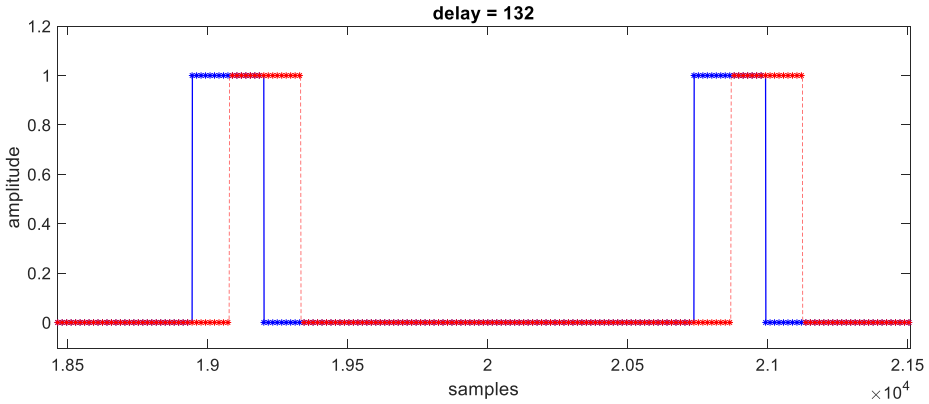

Figure 9. Example of reference (blue) and delayed received PPM symbols (red), with 132 sample delay.

residual delay of 132 simulation samples. However, with the 64-element nano-wire photon-counting detector arrays used in the DSOC receiver, each received pulse registers photon counts at random arrival times within each pulse. Examples of the photon counts and photon-arrival times for high-intensity and low-intensity signal cases without background are shown in Figure 7, where numerous single-photon and a few cases of two-photon counts can be seen for the high-intensity case of Figure 7a, but much fewer single-counts and even no photon-counts for a received pulse are evident in Figure 7b, over the short time interval corresponding to the five pulses shown.

The simulated photon-counts obtained with ideal photon-counting detectors with arbitrarily high bandwidth can be used to estimate the delay of the received PN-code pulses with respect to the reference pulses, as shown in Figure 10. If the reference pulses are approximated by the ideal count-intensities, as shown by the rectangular blue pulses in Figure 9, and the received signal is represented by the wide-band photon-detection pulses shown in red, then the delay in the received signal can be obtained by correlating the ideal reference pulse with the received signal, as in the RF case where this cross-correlation operation is known to be optimal in the presence of additive Gaussian noise. This results in the nearly ideal cross-correlation function shown in Figure 10a, where the difference between the peak of the reference-signal auto-correlation function (blue) and the peak of the cross-correlation function (red) can be used to determine delay by counting the number of simulation samples, since the simulation sample duration is known. With high-intensity pulses, the Gaussian approximation to Poisson counts is accurate as long as the variance of the Poisson counts is taken into account, in addition to the variance of the additive Gaussian noise.

However, with the lower count-intensities shown in Figure 10b, the cross-correlation function is distorted due to the granularity of the random photon counts and photon arrival times, potentially leading to larger delay estimation errors, even with high-rate sampling of 256 samples per pulse. For example, with an input delay of 132 samples in the simulation, the delay estimate with high-rate sampling and cross-correlation yields an accurate estimate of 132 samples when high-intensity pulses are used. However, low-intensity pulses, even without background interference and with the use of high-rate sampling, yields a slightly inaccurate estimate of 133 samples.

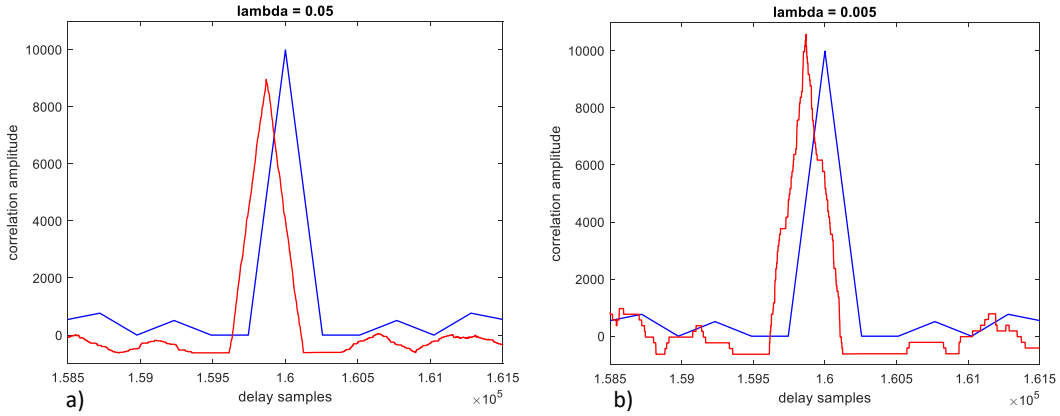

Figure 10. Reference and cross-correlation functions for high-rate sampling, no background interference: a) high energy pulses; b) low energy pulses.

The examples in Figure 10 refer to high-rate sampling simulating the performance of an ultra-wideband photon-counting detector. The simulation uses 256 high-rate samples to obtain the idealized correlation functions of Figure 10, but more realistic samples are also generated by summing the counts over 16 high-rate samples. An example of the summed samples is shown in Figure 11, where the high-rate samples were binned to obtain the large photon-counts in the received signal. The count intensity of the received delayed pulses is shown by the dashed green pulses, which are seen to contain the binned photon-counts as expected.

Since the ultra high-rate samples are not readily available, the receiver has to use the lower rate samples to determine delay, in a realistic configuration. Although the binning operation results in less resolution for determining the pulse arrival time, the random photon counts also tend to be smoothed by the binning operation, hence it is not clear what the impact of binning is on the accuracy of the delay estimates. In order to determine the effect of binning, we compute delay estimates via correlation for both high-rate and low-rate samples, and compare the mean value and standard deviation of the estimates to the ideal case represented by the high-rate samples.

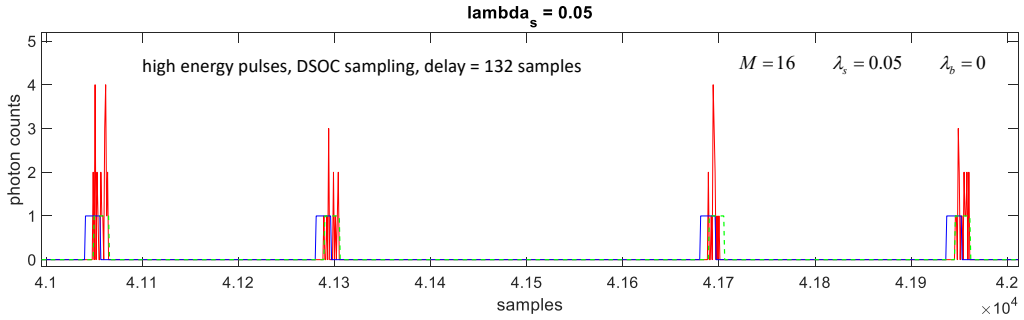

Figure 11. Simulated 500 ps samples for high-energy delayed pulses, by summing 16 high-rate samples. Dashed green pulses represent the count intensity of the received pulses, with a residual delay of 132 samples.

For this comparison of ultra high-rate sample cross-correlation with lower-rate cross correlation, we first consider PPM of order $M = 128$, with 256 samples per pulse (ultra-high rate sampling) and 16 samples per pulse assuming 8 ns pulse-widths [5]. A total 1.6×10^6 high-rate samples were used in the correlation estimates. The examples of cross-correlation functions for 10 independent runs presented in Figure 12 refer to average high-rate sample counts of 0.01 photons per sample.

Based on 10 independent runs of the cross-correlation estimator shown in Figure 12a, the mean delay estimate obtained from the ultra-high sampling rate estimator is 132.1 samples when the average sample photon-rate is 0.01 photons per pulse, while the rms delay error is 2.47 samples. Similarly, the coarse delay estimate for the lower rate samples is 128 instead of the input delay of 132 high-rate samples, for an error of 4 samples. These coarse estimates are the peaks of the correlation functions shown as the cyan plots in Figure 12b.

The correlation functions near the peak tend to be asymmetrical due to under-sampling, resulting in peaks that are closer to the reference peak than in the high-rate sampling case. This can be remedied by applying quadratic interpolation around the peak of the correlation function, using the peak correlation, and the two nearest samples on either side. The resulting quadratic interpolation functions are shown as the dashed red curves around the correlation peaks in Figures 12 and 13b, while the red asterisk denotes the interpolated delay estimate, in terms of high-rate samples. Using the quadratic interpolation function, the coarse estimates can be improved significantly, rivaling the accuracy of the high sample-rate estimator. For the example shown in Figure 13b, the mean value of the refined estimates is 130.82 samples, with an rms error of 2.18 high-rate samples. These examples suggest that performance comparable to that of the high-rate correlation estimator can be achieved with much lower rate and more realistic sampling, by applying the quadratic interpolation algorithm.

The results shown in Figure 12 are for the ideal case of no background photon or dark-count interference, both of which are typically present in real systems and may cause significant errors in the delay estimates. This case was also explored by increasing the background interference from zero to 0.001 photons per sample, yielding the plots shown in Figure 13.

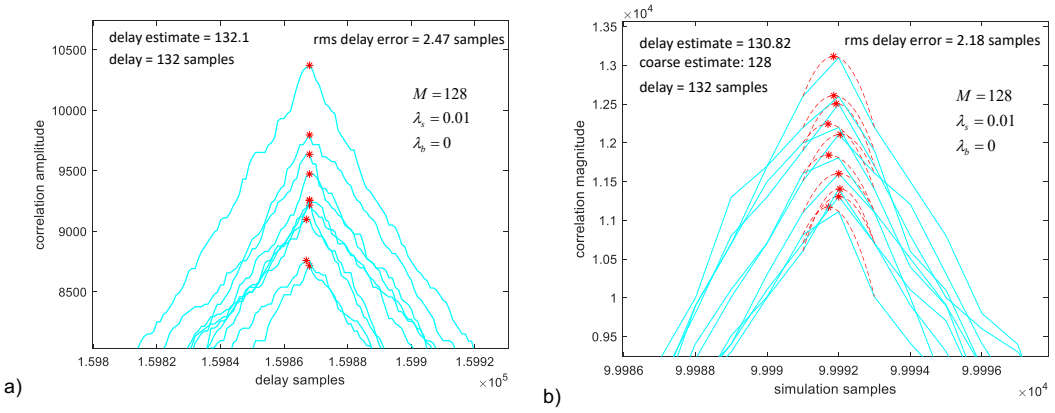

Figure 12. Cross-correlation functions for high-energy pulses, with no background photons: a) ultra-high rate sampling; b) DSOC receiver sampling with quadratic interpolation. Roughly 500 SCPPM symbols were used.

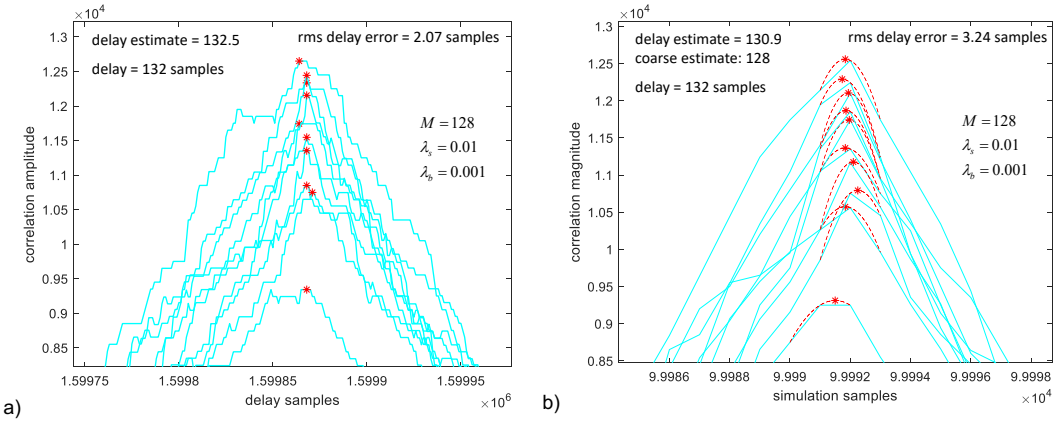

Figure 13. Cross-correlation functions for high-energy pulses, with moderate background photons: a) ultra-high rate sampling; b) DSOC receiver sampling with quadratic interpolation. Roughly 500 SCPPM symbols were used.

The above results indicate that correlation of the received photo-counts with a copy of the known SCPPM intensity distribution enables accurate estimates of round-trip delay with realistic samples of 500 ps as available from the DSOC receiver, with and without background radiation [5]. The standard deviation of 1 high-rate 500/16 = 31.25 ps sample corresponds to a range resolution of $\Delta R = c\tau/2 =$ 4.7 mm, where c is the speed of light, and the division by two accounts for the bounce from the lunar retro-reflector. Therefore, rms errors of 2–3 samples correspond to a range resolution of approximately 1–1.5 cm at the range of the Moon, with only 500 SCPPM symbols. Longer signal vectors yield correspondingly better estimates, therefore millimeter level accuracies should be achievable with a realistic deep-space optical receiver installed in the Hybrid RF/Optical telescope.

VI. Secret Key Distribution (SKD) Capacity with PPM Signals

We consider four different secret key capacities for the PPM transmitter. Here, we will model both our signal and our background photons as coherent states, so that they exhibit Poissonian statistics at a photon-counting receiver. By convention, we will refer to the transmitter as "Alice," the receiver as "Bob," and an eavesdropper as "Eve." We will assume that Alice is transmitting to Bob at a low average photon number, and that Bob receives some fraction η of the signal photons while the eavesdropper Eve receives the remaining $1 - \eta$. This way, Eve can be modeled as a beamsplitter. First, we will consider the secret key rate of a classical PPM protocol, where Alice inserts all of her signal photons in a single time slot, and Bob and Eve use standard photon counting measurements in each slot. We will then consider the capacity of a BB84-type PPM modulation, in which Alice randomly selects either the {*H, V*} or the {+, –} basis, and selects one of the two corresponding modes at random in which to insert all of her signal photons sent to Bob. Here, "*H*" and "*V*" respectively correspond to horizontal and vertical polarization, while "+" and "–" correspond to their rotations by 45 degrees. We will assume that these signal photons remain in their corresponding basis state en route to Bob. Finally, we will consider the

secret key capacity for each of these transmitters when both Bob and Eve are allowed to make an arbitrary quantum measurement.

We note that a more realistic approximation of weak background noise would be a thermal quantum state, with Bose-Einstein photon number statistics or Laguerre statistics in the presence of a signal pulse. However, when considering PPM signals, the dimension of the overall quantum state density operator grows exponentially in the number of time slots M. A pure coherent-state approximation of background noise allows us to more easily model the received quantum state as well as estimate the overall secret key capacity.

A. Standard PPM Transmitter with Photon Counting

In M-PPM modulation, Alice prepares a coherent state in one of M equiprobable time slots. Let N_S be the average number of signal photons in this slot, and N_b the average number of background photons. If we take X to be a random variable representing the index of the time slot, and let Y_x and Z_x be Bob's and Eve's respective photon counts in the time slot indexed by $x \in \{1, \ldots, M\}$, then Y_x is distributed as $Y_x \sim \begin{cases} Poiss\,(\eta N_s + N_b), & X = x \\ Poiss\,(N_b), & X \neq x \end{cases}$ and Z_x is distributed similarly, with η replaced by $1 - \eta$. Denote the resulting random vectors by $Y = [Y_1, \ldots, Y_M]$ and $Z = [Z_1, \ldots, Z_M]$.

The secret key capacity (in secret bits per PPM frame) is given as in Reference [6] by $C_{PPM} = I(X;Y) - I(X;Z)$. We can evaluate

$$I(X;Y) = H(Y) - H(Y|X) = H(Y) - \textstyle\sum_X P(X = x)H(Y|X = x), \tag{4}$$

where

$$\begin{aligned} &P(X = x) = 1/M \\ &H(Y|X = x) = (M-1)H\big(Poiss(N_b)\big) + H\big(Poiss(\eta N_S + N_b)\big) \\ &H(Y) = H\left(\left\{\frac{N_b^{\sum y_i}}{M y_1! \cdots y_M! exp(MN_b + \eta N_S)} \sum \left(\frac{\eta N_s + N_b}{N_b}\right)^{y_i}\right\}\right). \end{aligned} \tag{5}$$

When M, N_b, and N_S are small, we can compute these entropies explicitly. Otherwise, we approximate the Poisson distributions as Gaussians, and use the approximation [7]

$$\begin{aligned} I(X;Y) \approx\ & \log_2 M \\ & -E_{v_1|\boldsymbol{x_1}} \log_2 \left[1 + (M-1)\sqrt{(\rho_0 + \rho_+)/\rho_+}\, \exp\left(\frac{\rho_0\rho_+ - 2\rho_+\sqrt{\rho_0}v_1 - \rho_0 v_1^2}{2(\rho_0 + \rho_+)}\right)\right] \end{aligned} \tag{6}$$

where $\rho_0 = (\eta N_S)^2/N_b$, $\rho_+ = \eta N_S$, and $v_1 | \boldsymbol{x_1} \sim N\left(\sqrt{\rho_0}, \frac{\rho_0 + \rho_+}{\rho_+}\right)$.

These computations are all mimicked for $I(X;Z)$ by replacing η with $1-\eta$. Figure 14 shows the secret key capacities for Standard PPM, as a function of the fractional received average signal photons (η) per PPM pulse.

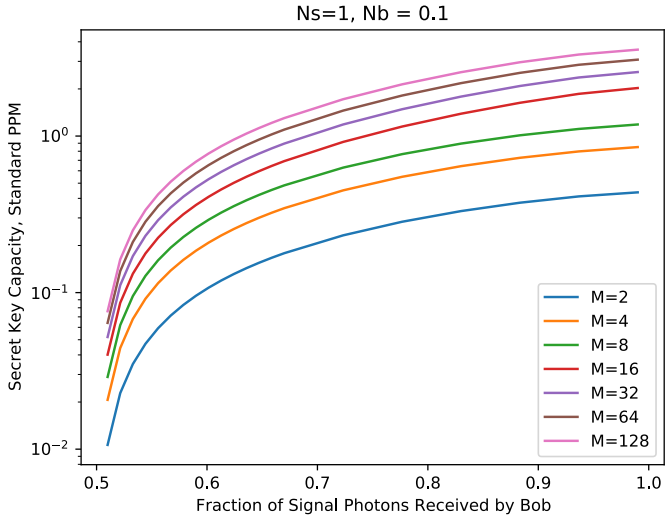

Figure 14. Secret key capacities for Standard PPM (in secret bits per PPM frame) versus fractional received signal photons. Results are plotted for average number of signal photons per pulse N_S = 1, and average number of background photons per pulse N_b = 0.1, for varying PPM orders (M).

B. BB84 Combined with PPM and Photon Counting

When the PPM signal is additionally modulated by Alice randomly choosing one of the polarizations {H,V, +, –} in which to prepare her signal photons, both Bob and Eve can randomly select one of the two bases {H,V} and {+, –} in which to measure their photons. We assume that Alice and Bob perform sifting, only keeping PPM frames in which Bob measured in the same basis in which Alice prepared her signal photons, which will occur 50% of the time. Eve is privy to the discussion between Alice and Bob, and will have used the same basis for half of the PPM frames that they agreed on: that is, 25% of the time. Thus, the secret key capacity for Alice and Bob becomes $C_{BB84-PPM} = \frac{1}{2} I(X;Y) - \frac{1}{4} I(X;Z)$, where now M is replaced by $2M$ and N_b is replaced by $N_b/2$ in our calculations of $I(X;Y)$ and $I(X;Z)$, since we are effectively doubling the number of modes that we are measuring (two polarization directions per time slot), and we should expect only half the total background photons in each orthogonal polarization direction of a given basis. Figure 15 shows the behavior of the secret key capacities for BB84-PPM, as a function of the fractional received average signal photons received by Bob per PPM symbol.

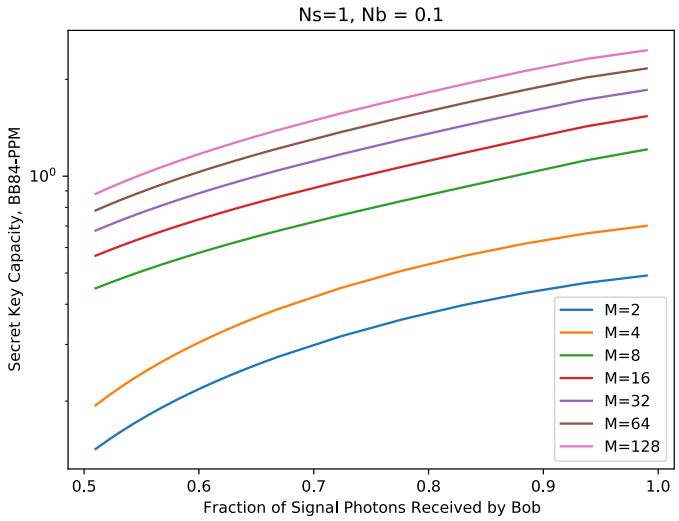

Figure 15. Secret key capacities for BB84-PPM versus fractional received signal photons. Average number of signal photons per pulse is $N_S = 1$, and average number of background photons per time slot is $N_b = 0.1$. PPM order is denoted by M.

C. Standard PPM and BB84-PPM with Optimal Quantum Measurements

In full generality, Bob and Eve should be allowed to perform any theoretically possible quantum measurement. To find the ultimate secret key capacity in the standard PPM case, we must therefore express the transmitted signal as a quantum state. In our case, if Alice places her signal in the x^{th} time slot, the state received by Bob is a tensor product of coherent states, namely $|\psi_Y\rangle_x = |\alpha_b\rangle_1 \otimes \ldots \otimes |\alpha_S\rangle_x \otimes \ldots \otimes |\alpha_b\rangle_M$, where $|\alpha_b\rangle$ is the "background noise" coherent state ($\alpha_b = \sqrt{N_b}$) and $|\alpha_S\rangle$ is the "signal" coherent state, with $\alpha_S = \sqrt{\eta N_S + N_b}$ for Bob and $\alpha_S = \sqrt{(1-\eta)N_S + N_b}$ for Eve. The quantum secret key capacity is given by Reference [8] $C_{Q-PPM} = I(X;Y)_\rho - I(X;Z)_\rho$, where ρ_{XYZ} is the quantum state shared by Alice, Bob, and Eve. By modeling the signal and noise as coherent states, we guarantee that the state received by Bob is pure when conditioned on the classical variable X (even after tracing out Eve's subsystem). As a result, we can compute

$$I(X;Y)_\rho = H(Y)_\rho - \sum_x P(X=x)\, H(|\psi_Y\rangle\langle\psi_Y|_x) = H(Y)_\rho \tag{7}$$

Here, $H(Y)_\rho = -Tr(\rho_Y \log_2 \rho_Y)$ is the von Neumann entropy, where ρ_Y results from tracing out the X and Z subsystems from ρ_{XYZ}. Explicitly, we have $\rho_Y = \sum_x P(X=x)\, |\psi_Y\rangle\langle\psi_Y|_x$. For computational purposes, we only compute C_{Q-PPM} when M is sufficiently small, and we approximate each $|\psi_Y\rangle_x$ by its projection onto the space spanned by tensor products of Fock states $|n_1\rangle_1 \otimes \ldots \otimes |n_M\rangle_M$, where each n_M is also small. This is a reasonable approximation of the state when N_S and N_b are small. As before, our methods for computing $I(X;Z)_\rho$ are the same as those for computing $I(X;Y)_\rho$.

The capacity of BB84-PPM with general quantum measurements is computed similarly, except that now our coherent background noise state is $|\alpha_b\rangle^{\otimes 2}$ with $\alpha_b = \sqrt{N_b/2}$, since each time slot will include measurements in two polarization modes, each of which will

have half the background photons. Also different is the fact that Alice now has four different types of coherent signal states, each corresponding to one of {H,V, +, –}. Explicitly, these will be:

$$\begin{aligned} |\alpha_H\rangle &= |\alpha_{11}\rangle \otimes |\alpha_{12}\rangle, \\ |\alpha_V\rangle &= |\alpha_{12}\rangle \otimes |\alpha_{11}\rangle, \\ |\alpha_+\rangle &= |\alpha_{21}\rangle \otimes |\alpha_{22}\rangle, \\ |\alpha_-\rangle &= |\alpha_{22}\rangle \otimes |\alpha_{21}\rangle, \end{aligned} \tag{8}$$

where $\alpha_{11} = \sqrt{\eta N_S + N_b/2}$, $\alpha_{12} = \sqrt{N_b/2}$, $\alpha_{21} = j\sqrt{\eta N_S/2} + \sqrt{N_b/2}$, $\alpha_{21} = -j\sqrt{\eta N_S/2} + \sqrt{N_b/2}$. Now the states $|\psi_Y\rangle_x$ are replaced by $|\psi_Y\rangle_{x,s}$, where $x \in \{1, \ldots, M\}$ corresponds to the time slot index and $s \in \{H, V, +, -\}$ corresponds to the signal type. Each of these states is equiprobable, with $P\big((X,S) = (x,s)\big) = 1/4M$. Likewise, the states $|\psi_Z\rangle_{x,s}$ received by Eve are constructed the same way, but with η replaced by $1 - \eta$. Figure 16 shows the behavior of the secret key capacities for Standard PPM and BB84-PPM as a function of the fractional received average signal photons received by Bob per PPM symbol, for both photon counting and generalized quantum measurements.

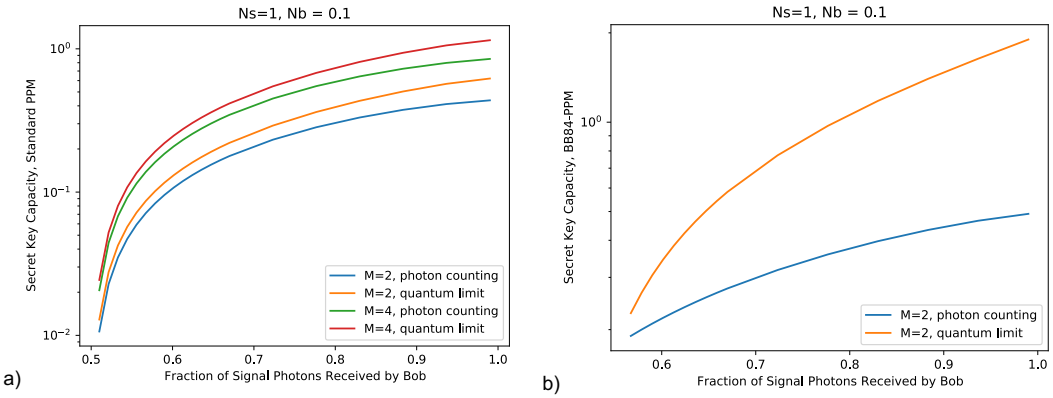

Figure 16. Secret key capacities for a) Standard PPM and b) BB84-PPM models, versus the fractional received signal photons per PPM symbol for both photon counting and general quantum measurements. Plotted at low PPM orders (*M*) for average signal photons per pulse N_s = 1, and average number of background photons per time slot N_b = 0.1.

D. Explicit Code for Secret Key Distribution for Standard PPM

We show how to construct a code capable of performing secret key distribution at the optimal rate for standard M-PPM. Setting $M = 2^m$, begin with a linear encoder E: $\{0,1\}^k \rightarrow \{0,1\}^{mn} = \{0, 1, \ldots, M-1\}^n$, where we have identified the elements $\{0, \ldots, M-1\}$ with those of $\{0,1\}^m$. Here we select k and n so that k/mn is approximately equal to $I(X;Y)$. This means that for k and n large enough, there is a corresponding decoder D which maps Bob's received output of the n channel uses back to its corresponding vector in $\{0,1\}^k$ with low probability of error. For the sake of argument, assume that $\ell := k \cdot \frac{I(X;Z)}{I(X;Y)} = mn \cdot I(X;Z)$ is an integer. We construct our code as follows: identify $\{0,1\}$

with GF(2), so that $\mathrm{GF}(2)^{\mathrm{k}} = \mathrm{GF}(2)^{\ell} \times \ldots \times \mathrm{GF}(2)^{\ell}$ with $\mathrm{GF}(2)^{\ell}$ repeated $\frac{I(X;Y)}{I(X;Z)}$ times. Let L be the subspace of $\mathrm{GF}(2)^{\mathrm{k}}$ consisting of vectors of the form $[\boldsymbol{v}\ \boldsymbol{v} \ldots \boldsymbol{v}]$, with $\boldsymbol{v} \in \mathrm{GF}(2)^{\ell}$. Clearly this subspace is itself isomorphic to $\mathrm{GF}(2)^{\ell}$ as a vector space. As such, it partitions $\mathrm{GF}(2)^{k}$ into $2^{k-\ell} = 2^{mn(I(X;Y)-I(X;Z))}$ distinct cosets, which we label as the bit strings $c \in \{0,1\}^{mn(I(X;Y)-I(X;Z))}$ and identify with a coset representative $\mathbf{v^c} = [\boldsymbol{v_1^c}\ \boldsymbol{v_2^c} \ldots \underbrace{\boldsymbol{v_k^c}}_{\ell}]$.

Furthermore, we argue that since we are using PPM modulation, we may take our encoder E such that when restricted to the set of vectors in L, the resulting code achieves capacity for the channel to Eve. Consider, for instance, taking the encoder to be in the form $[E_1 E_2 \ldots \underbrace{E_k}_{\ell}]$, where each E_i: $\{0,1\}^{\ell} \to \{0,1\}^{mn\ell/k}$ is an identical linear encoder which achieves capacity for Bob (with perhaps some modifications to our code length). Then E is a repetition code when restricted to the vectors $[\boldsymbol{v}\ \boldsymbol{v} \ldots \boldsymbol{v}]$, which can be made to achieve the capacity for the channel from Alice to Eve.

Alice now selects one of these cosets c uniformly at random, which represents $mn\big(I(X;Y) - I(X;Z)\big)$ secret bits. She also selects a uniformly random vector $\mathbf{v} = [\boldsymbol{v}\ \boldsymbol{v} \ldots \boldsymbol{v}] \in \boldsymbol{L}$, which represents another $\ell = mn \cdot I(X;Z)$ bits**.** She takes the sum $\mathbf{v^c} + \mathbf{v}$, which corresponds to a sequence in $\{0,1\}^{\mathrm{k}}$, which she encodes with E into n PPM channel uses and sends to Bob (and Eve). We see that in order for Eve to learn all of the secret bits, she must implicitly learn $\mathbf{v}$, which in and of itself requires a rate of classical communication between Alice and Eve of $I(X;Z)$. But this is Eve's capacity, and were she to learn this, she could not learn the additional bits associated to the coset c.

We must argue that Eve cannot learn *any* information about the coset c. By our encoder design, Eve's outputs Z are approximately uniformly distributed over a typical set of size $\sim 2^{mn \cdot I(X;Z)}$, and for any coset c, Eve's outputs Z_c must be probabilistically mapped to a subset of this typical set. We argue that the distribution of the Z_c is the same as that for all the Z. For each c, then we effectively form a new codebook $\{\mathbf{v^c} + \mathbf{v}\}_{\mathbf{v} \in L}$. Again, by the construction of our encoder and the fact that it achieves capacity for Eve on L, we see that it also achieves capacity when restricted to any one of these codebooks, provided that Eve knows $\mathbf{v^c}$. Since the $\mathbf{v}$ are uniformly distributed over a set of size $2^{mn \cdot I(X;Z)}$, the output distribution of the Z_c will also be approximately uniform over a typical set of this size. This implies that the distribution of the Z_c is approximately identical to that of all the outputs Z, meaning that $H(Z|c) \approx H(Z)$, which immediately implies that $I(c;Z) \approx 0$. In other words, Eve has no information about the $mn\big(I(X;Y) - I(X;Z)\big)$ bits encoding the coset c.

Since this is a linear code, Bob can easily decode it by multiplying the orthogonal complement of the generator matrix of L, which is the parity matrix $\mathbf{H}$. This cancels out the $\mathbf{v}$ component of Alice's message $\mathbf{v^c}$+$\mathbf{v}$, leaving $\mathbf{Hv^c}$. If we can choose the coset representatives to have unique images under $\mathbf{H}$, Bob can decode quickly. This method allows Alice and Bob to use standard capacity-achieving linear codes and encoders as components to build a code that achieves the secret key capacity using standard PPM modulation.

VII. Summary and Conclusions

In this article, we examined the potential application of the five retro-reflectors left on the Moon by the Apollo missions, together with the Hybrid RF/Optical Receiver and a corresponding laser ground transmitter to emulate the photon-starved optical deep-space channel. Extremely short Earth-to-Moon round-trip light-times together with planetary rotation, orbital dynamics, atmospheric turbulence and space-loss due to the "inverse distance-to-the-fourth" power law will enable rapid development and testing of new techniques and algorithms for future communications, ranging and science applications in a realistic environment. Here, we developed accurate analytic models of atmospheric turbulence, background radiation, and optical SCPPM modulation to help evaluate system performance for communications, ranging, and secret key distribution protocols of potential interest for future human exploration and robotic missions in the solar system. It was shown that optical SCPPM modulation transmitted from the ground to the retro-reflectors could be used to emulate communications, ranging, and SKD experiments in the presence of turbulence and background radiation, achieving performance levels consistent with nominal requirements expected for future deep-space exploration.

Acknowledgment

The authors would like to thank Kenneth Andrews of Section 332, for providing the MATLAB code to generate the SCPPM symbols used in the simulation.

References

[1] G. J. Baker, R.S. Benson, "Gaussian beam scintillation on ground to space paths: the importance of beam wander," *Proceedings of SPIE,* vol. 5550, 2004.

[2] J. A. Shaw, "Modeling infrared lunar radiance," *Optical Engineering,* vol. 38, no. 10, October 1999.

[3] M. Zhu, Y. Li, J. D. Ellis, "Polarization model for total internal reflection-based retroreflectors," *Optical Engineering,* vol. 53, no. 6, June 2014.

[4] CCSDS 142.0-B-1, Optical Communications Coding and Synchronization, Blue Book, 19 August 2019. https://public.ccsds.org/Pubs/142x0b1.pdf

[5] M. Srinivasan, R. Rogalin, N. Lay, M. Shaw, A. Tkacenko, "Downlink receiver algorithms for deep-space optical communications," *Proceedings of SPIE,* vol. 10096, 2017.

[6] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975. doi: 10.1002/j.1538-7305.1975.tb02040.x.

[7] S. Dolinar, D. Divsalar, J. Hamkins and F. Pollara, "Capacity of PPM on Gaussian and Webb channels," *2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060)*, Sorrento, Italy, 2000, pp. 410– . doi: 10.1109/ISIT.2000.866708.

[8] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, January